# DsiN-Praxisreport 2018
# Mittelstand@IT-Sicherheit

Schirmherrschaft:

Bundesministerium
des Innern, für Bau
und Heimat

DsiN Deutschland sicher im Netz

Dr. Daniel Holz

Dr. Michael Littger

# Dialog für Sicherheit im Mittelstand – mit allen Akteuren!

Der neu aufgelegte DsiN-Praxisreport 2018 wirft ein Schlaglicht auf die aktuelle IT-Sicherheitslage des deutschen Mittelstands. Grundlage sind die Erhebungen des DsiN-Sicherheitschecks, der 2017 auf dem Digital-Gipfel vorgestellt wurde. Er gibt einen direkten Einblick in den Maschinenraum deutscher Unternehmen. Im Fokus stehen Themen aus dem betrieblichen Alltag, die zunehmend von einer sicheren und störungsfreien IT abhängig sind: von der digitalen Ausgestaltung des Arbeitsplatzes über Infrastruktur bis zur Vernetzung eines Betriebs mit Partnern.

Der Report zeigt die Praxis der Mitarbeiter und Entscheider auf, die durch ihre Tätigkeiten und Handlungen – jeden Tag – über IT-Sicherheit und Datenschutz ihres Unternehmens entscheiden. Wie also steht es um IT-Sicherheit in der Praxis, welche Vorkehrungen finden Akzeptanz in der Praxis – und welche Hemmnisse bestehen in der Umsetzung? Im Kern zeichnen sich zwei Entwicklungen ab:

- Die Digitalisierung im Mittelstand stellt wachsende Anforderungen an die Sicherheit. Dies gilt für organisatorische Vorkehrungen bis zur Umsetzung einzelner Maßnahmen auf Mitarbeiterebene. Diesen neuen Herausforderungen kommen Unternehmen heute - aus unterschiedlichen Gründen - nur teilweise und punktuell nach. Bei kleineren Betrieben bestehen darüber hinaus oftmals Defizite bei grundlegenden technischen Sicherheitsvorkehrungen.

- Der wachsenden Kluft von Anspruch und Wirklichkeit in der IT-Sicherheit stehen neue Möglichkeiten gegenüber, um Schwachstellen entgegenzuwirken. Der Report zeigt, welche konkreten Angebote bestehen, um Betriebe auf dem Weg zu einem zeitgemäßen Management von Informationssicherheit zu unterstützen. Aber auch Hürden werden deutlich, die Unterschiede zwischen Branchen und Unternehmensgrößen erkennen lassen.

Mit dem Report werden neue Lösungswege aufgezeigt, wie eine Verbesserung der IT-Sicherheit in der Praxis erreicht werden kann. Es geht um Maßnahmen, die auf solche Schwachstellen und Defizite eingehen, und im Praxisreport beschrieben werden. Im fünften Kapitel wird daraus ein Drei-Punkte-Plan abgeleitet, um IT-Sicherheit über digitale Aufklärung im Mittelstand voranzutreiben.

Ganz im Sinne von Deutschland sicher im Netz geht es im vorliegenden Praxisreport um wirksame Hilfe zur Selbsthilfe. Das kann nur im Verbund aller Akteure gelingen. Im neuen *Deutschland Dialog für digitale Aufklärung* von DsiN werden Bedarfe identifiziert, um im Mittelstand neue Projekten und Angebote bereit zu stellen.

Wir wünschen Ihnen eine anregende Lektüre!

**Dr. Daniel Holz**
Stellvertretender DsiN-Vorstandsvorsitzender
und Geschäftsführer der SAP Deutschland SE & Co. KG

**Dr. Michael Littger**
DsiN-Geschäftsführer

# Ziel und Design des Praxisreports

Dem Praxisreport liegt eine repräsentative Erhebung bei Mitarbeitern und leitenden Angestellten kleiner und mittlerer Unternehmen zu Grunde: Die Ergebnisse leiten sich aus ihren Angaben und Erfahrungen ab, die anhand eines Fragenkatalogs zu 24 Themenfeldern gestellt wurden. Insgesamt wurden 1.705 abgeschlossene Erhebungen im Zeitraum von Juni 2017 bis Juli 2018 durchgeführt und ausgewertet.

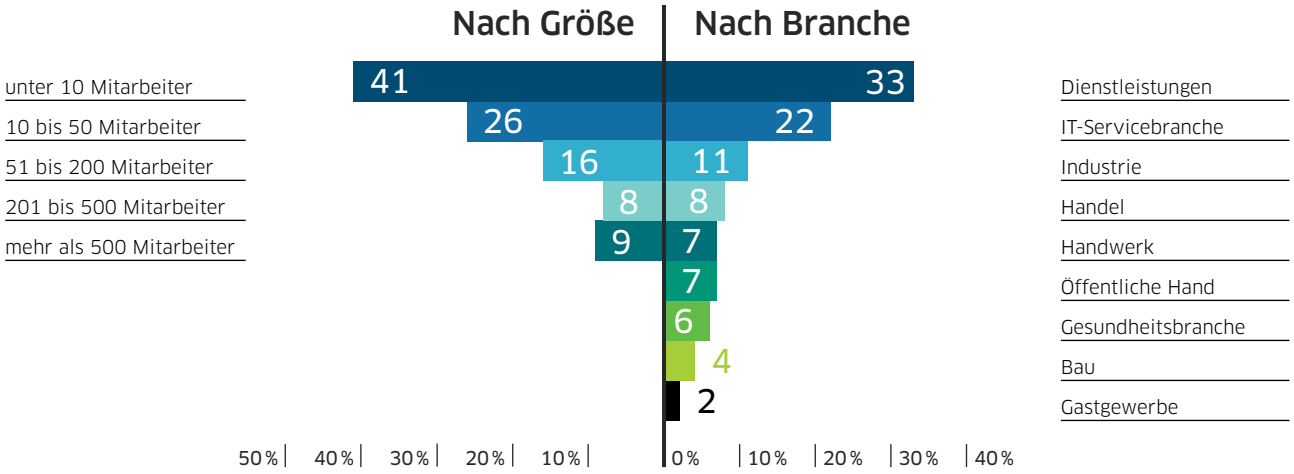
Die Studie umfasst auch Unternehmen mit weniger als 10 Beschäftigten, die mit 41 Prozent sogar die größte Gruppe der Beteiligten darstellt, gefolgt von Kleinunternehmen mit bis zu 50 Beschäftigten mit 26 Prozent. 16 Prozent der Teilnehmer der Studie stammen aus Unternehmen mit einer Mitarbeiterzahl von 51 bis 200. Unternehmen mit 201 bis 500 Beschäftigten sind 8 Prozent der Teilnehmer zuzuordnen. Damit zählen über 90 Prozent aller befragten Unternehmen zum Mittelstand anhand des zentralen Größenkriteriums von bis zu 500 Beschäftigten.

Hinsichtlich der Zuordnung auf konkrete Branchen gehört rund ein Drittel dem Bereich Dienstleistung (33 Prozent) an. Die ITK-Branche ist mit rund 22 Prozent der Teilnehmer vertreten. Industrie (11 Prozent) und Handel (8 Prozent) bilden zusammen ein weiteres Fünftel der Befragten. Mit zusammen gut 11 Prozent sind Handwerk (7 Prozent) und Bau (4 Prozent) vertreten. Ferner haben Vertreter der Gesundheitsbranche (6 Prozent), der öffentlichen Hand (7 Prozent) sowie dem Gastgewerbe (2 Prozent) teilgenommen.

Mehr als die Hälfte der Befragten gab an, für IT-Sicherheit zertifiziert oder zumindest Ansprechperson für dieses Thema zu sein. Der Praxisreport schließt an die Reihe des DsiN-SicherheitsMonitor der Jahre 2011 bis 2016 und verweist im Einzelfall auf diese Vorgängerstudie.

**Aufteilung der befragten Unternehmen**

**Abb. 1**



# Inhaltsverzeichnis

# Zentrale Ergebnisse

**Mittlerweile ist knapp die Hälfte der an der Umfrage beteiligten KMU zur Erkenntnis gelangt, dass ihre Betriebsabläufe unmittelbar von der IT-Sicherheit abhängen. Dennoch werden bewährte Einzelmaßnahmen weiterhin vernachlässigt. Auch eine adäquate Risikoermittlung und Notfallpläne bleiben häufig ganz aus. Bei der Detektion verhalten sich die KMU passiv – oder verlassen sich auf die eigenen Mitarbeiter*, ohne die nötigen Schulungen vorzunehmen.**

Während weite Teile des Mittelstands erkannt haben, dass sich wirtschaftlicher Erfolg heute am Faktor IT-Sicherheit bemisst, herrscht eine erstaunliche Unkenntnis, wenn es um das potenzielle Interesse Dritter an ihrem Know-how geht. Wie sehr hier Umsicht, Diskretion und Schnelligkeit gefragt sind, hat sich unter den beteiligten Unternehmen noch nicht herumgesprochen.

Die Mehrheit der befragten KMU ist überzeugt, noch nie Opfer eines Cyber-Angriffs geworden zu sein. Die Dunkelziffer dürfte höher liegen: denn bei der Detektion von Angriffen bleibt ein Drittel absolut passiv, und ein weiteres Drittel verlässt sich auf die eigenen Mitarbeiter für das Erkennen von Angriffen.

Mehr als 40 Prozent der KMU verzichten auch 2018 noch auf regelmäßige Aktualisierungen ihrer Software und Systeme. Auch Einzelmaßnahmen wie der Schutz der E-Mail Kommunikation haben sich nur geringfügig und auf einem zu niedrigen Niveau verbessert. Und 22 Prozent der an der Untersuchung beteiligten Unternehmen verzichten auf die Durchführung regelmäßiger Datensicherungen oder gar ganz auf Datensicherungen.

Das mag auch daran liegen, dass die Risikoermittlung in Betrieben grundsätzlich vernachlässigt wird – 70 Prozent der befragten KMU begnügen sich bestenfalls mit einer einmaligen Ermittlung ihrer individuellen Risikosituation. Diese passive Haltung spiegelt sich auch in einem weiterhin niedrigen Niveau beim Erstellen von Notfallplänen wider.

Bei der Verantwortung für IT-Sicherheit sehen die befragten Unternehmen dieses Reports vor allem die Geschäftsleitungen in der Pflicht. Aber auch die Mitarbeiter sollen Verantwortung tragen. Vertrauen ist zweifellos ein hohes Gut, doch handelt es sich mit Blick auf die Fakten wohl eher um Vertrauensseligkeit: Nicht einmal jedes fünfte Unternehmen sieht verpflichtende Sicherheitsschulungen für sein Personal vor.

Und dabei schreitet der Digitalisierungsgrad auch im Mittelstand voran: Bereits mehr als 40 Prozent der beteiligten KMU nutzen das Internet für den Vertrieb ihrer Produkte. Hingegen nutzt nur ein Fünftel Penetrationstests, um die Sicherheit ihrer Plattformen zu prüfen. Zudem setzt die Mehrheit der KMU nach wie vor noch nicht auf Cloud-Dienste, weil viele über unzureichende Kenntnisse hinsichtlich der Sicherheitsanforderungen und rechtlichen Rahmenbedingungen für die Nutzung verfügt.

Die Erkenntnisse dieses Praxisreports verlangen nach konkreten Maßnahmen, die wir in unserem Drei-Punkte-Plan präsentieren werden.

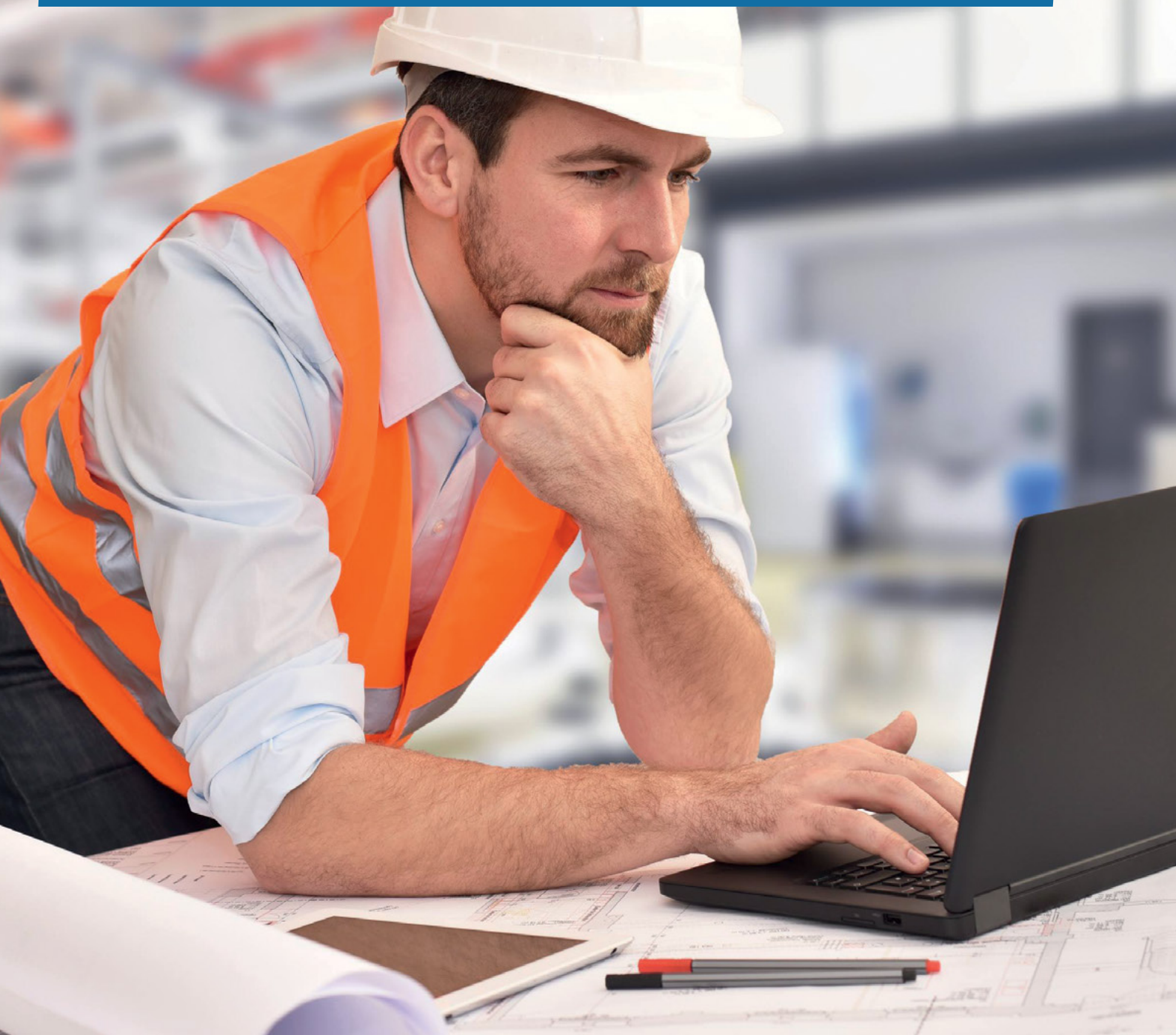
* Obwohl aus Gründen der Lesbarkeit im Text die männliche Form gewählt wurde, beziehen sich die Angaben stets auf die Angehörigen aller Geschlechter.

## Kapitel 1

# Mittelstand digital: Weckruf für IT-Sicherheit

Die digitale Transformation wirkt heute auf fast jedes kleine und mittlere Unternehmen. Der Praxisreport Mittelstand@IT-Sicherheit wirft ein Schlaglicht auf die aktuellen Herausforderungen der IT-Sicherheit und des Datenschutzes – und wie Mitarbeiter und Entscheider damit heute umgehen.

Erst aus dieser Bestandaufnahme kann ein Lagebild über Defizite und Bedarfe entstehen, das in Zukunft durch gezielte Angebote zu einer Verbesserung der IT-Sicherheit führen kann.



# IT-Sicherheit in der Praxis – Schutzbedarf und Risiko

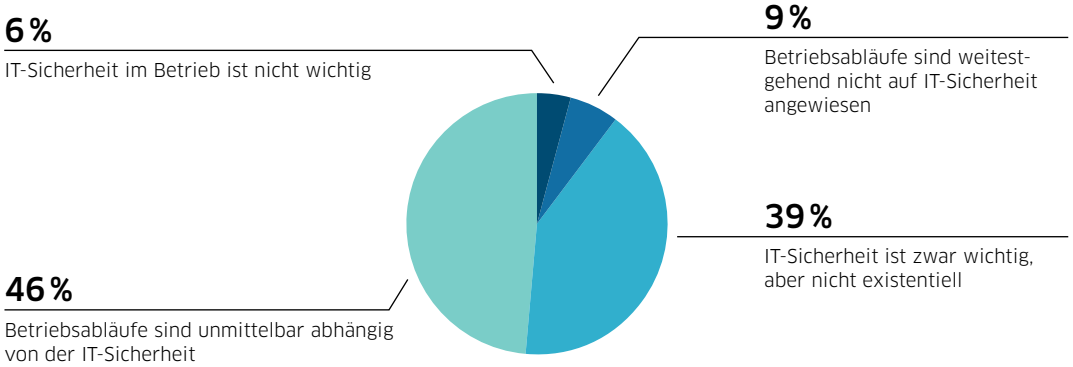
**Am Anfang jeder Bestandsaufnahme zur IT-Sicherheitslage steht die Analyse der Risiken und Schutzbedarfe. Sie umfasst Aspekte der Integrität, Vertraulichkeit und Verfügbarkeit von Informationen und Informationssystemen und ist grundlegend für reibungsfreie Betriebsabläufe, die vielfach schon digitalisiert und vernetzt sind. Des weiteren geht es um den Schutz vor unbefugter Einsicht und Manipulation durch Dritte – sowie um die Erfüllung neuer rechtlicher Anforderungen an IT-Sicherheit (Compliance). Wie sehen Unternehmen im Mittelstand ihre eigene Sicherheitslage und Schutzbedürftigkeit?**

## Fast jedes zweite Unternehmen abhängig von IT-Sicherheit

Die zunehmende Vernetzung und Digitalisierung im Mittelstand stärkt auch das Bewusstsein über die eigene Abhängigkeit von IT-Sicherheit und funktionierenden Systemen. Bei den befragten Unternehmen sahen 85 Prozent mindestens eine hohe Wichtigkeit der IT-Sicherheit, 46 Prozent sprachen sogar von einer direkten Abhängigkeit (Abb. 2):

**DsiN-Praxisreport:** Welche Abhängigkeit zwischen dem Erfolg des Unternehmens und der Integrität, Vertraulichkeit oder Verfügbarkeit von Informationen im Sinne von IT-Sicherheit besteht?

**Abb. 2**



Ein direkter Zusammenhang zwischen dem wirtschaftlichen Wohlergehen des eigenen Betriebs und IT-Sicherheit wächst mit steigender Unternehmensgröße (Abb 2a). So sehen mehr als die Hälfte der Mitarbeiter und Entscheider großer mittelständischer Betriebe einen Zusammenhang, während dies bei Kleinstunternehmen nur gut jeder Dritte Beschäftigte ist (38 Prozent).

Abb. 2a

**DsiN-Praxisreport:** Sehen Sie einen direkten Zusammenhang zwischen wirtschaftlichem Wohlergehen und IT-Sicherheit? Zustimmung bei …

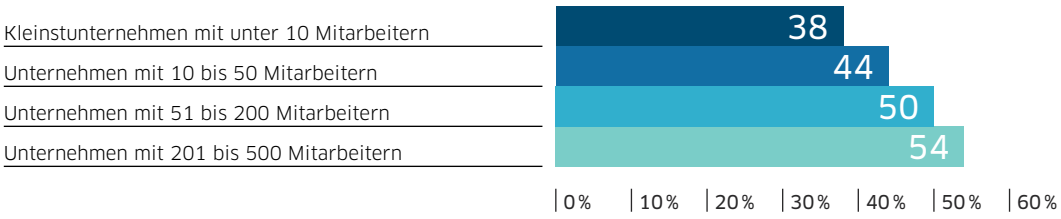
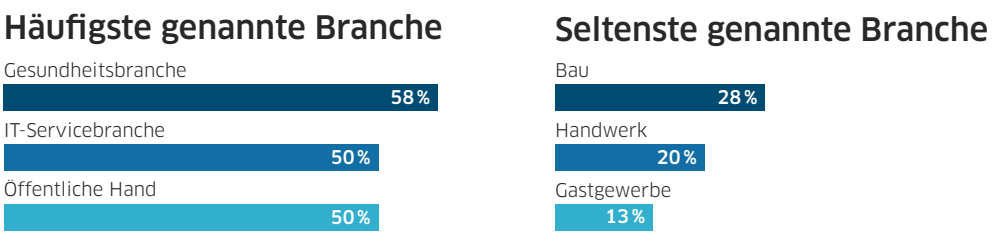



Abb. 2b

**DsiN-Praxisreport:** Wenn Sie einen direkten Zusammenhang von wirtschaftlichem Wohlergehen und IT-Sicherheit sehen, welcher Branche gehören Sie an …




Auffällig ist, dass der Zusammenhang zu IT-Sicherheit im Gesundheitswesen, IT-Servicebranche und öffentlicher Hand relativ präsent ist (Abb 2b). Im Gastgewerbe, Handwerk und Bau wird dem Zusammenhang keine besondere Relevanz eingeräumt. Dies könnte auf einen subjektiv geringeren Grad an Digitalisierung und Umgang mit sensiblen Daten in diesen Branchen zurückzuführen sein, aus dem heraus auf die Abhängigkeit des Betriebes von digitalisierten Betriebsabläufen geschlossen wird.

Aber auch bei den Spitzenreitern wird ein Zusammenhang nur bei weniger als zwei von drei Unternehmen gesehen. Hier bleibt abzuwarten, wie mit steigender Vernetzung von Lieferanten und Kunden diese Einschätzung in Zukunft ausfällt. Schon heute werden nur wenige Betriebe bei einem Ausfall der IT ihren Betrieb ohne Beeinträchtigung aufrechterhalten können.

## Jedes dritte Unternehmen fürchtet Angriff auf vertrauliche Daten

Der deutsche Mittelstand verfügt mit über 2.000 Hidden Champions in vielen Bereichen über herausragendes Know-how, das weltweit die Wettbewerbsfähigkeit sichert. Grundsätzlich könnte aber jedes Unternehmen durch einen Angriff auf Daten und die IT-Systeme enormen Schaden erleiden. Die Haltung des Mittelstands gegenüber möglichen Angriffen ergibt ein differenziertes Bild (Abb. 3).

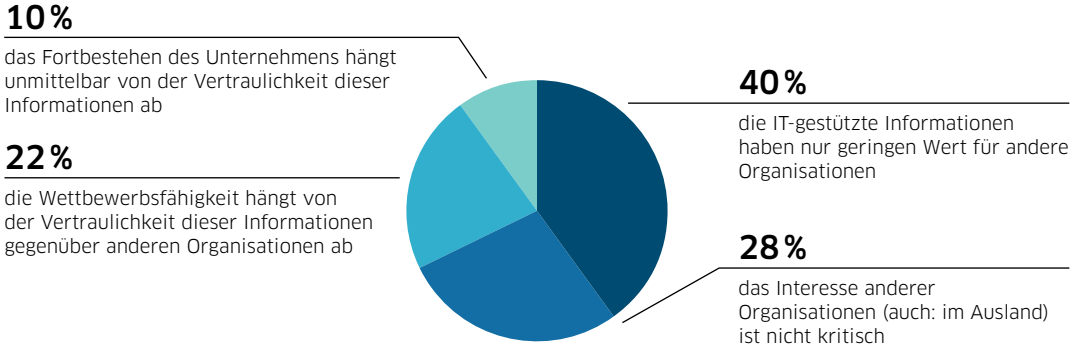
Im Ergebnis zeigen 10 Prozent der Unternehmen an, dass sie durch den Angriff auf ihre Datenbestände ihre Existenz unmittelbar gefährdet sehen. Für fast ein Drittel hingegen hängt die Wettbewerbsfähigkeit von der Sicherheit ihrer vertraulichen Daten ab.

Andererseits erachten 68 Prozent der KMU ihr eigenes Know-how als nicht schützenswert. Damit empfindet sogar eine Mehrheit keinen besonderen Schutzbedarf ihres Know-hows im Hinblick auf das eigene wirtschaftliche Wohlergehen. Dieses Ergebnis mag zunächst weniger überraschen, da eine Vielzahl von Betrieben über keine „sensiblen" oder „kritischen" Daten verfügen mag. Gleichwohl können Datenabflüsse bei allen Betrieben zu folgeschweren Beeinträchtigung führen. Dieser Zusammenhang könnte auf den ersten Blick vernachlässigt worden sein.

In dieser Sorglosigkeit deutet sich eine gewisse gutgläubige Haltung an („es wird schon gut gehen") sowie auch die Einstellung, dass sich „niemand für meine Informationen interessiert". Hier könnte digitale Aufklärungsarbeit ansetzen: Es gilt, die potenziellen Risiken praxisnah zu vermitteln, insbesondere bei Klein- und Kleinstunternehmen. Vor dem Hintergrund sollten Aufklärungsangebote Angestellte sowie auch Leitende einbinden, um den Wert der Datenintegrität übergreifend zu vermitteln.

**DsiN-Praxisreport:** Wie schätzen Unternehmen die Gefährdung der Vertraulichkeit und Integrität ihrer IT-gestützten Informationen durch Angriffe anderer Organisationen (auch der Konkurrenz)?

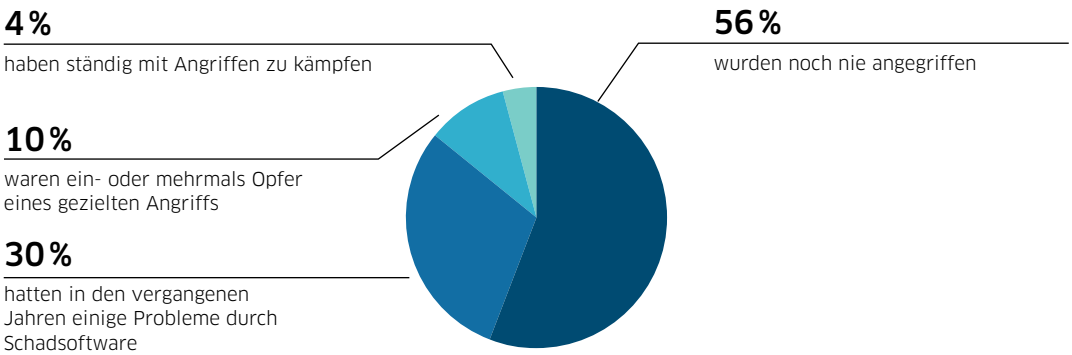
**Abb. 3**



## 44 Prozent der Unternehmen von Angriffen betroffen

Für betroffene Betriebe kann ein erfolgter Angriff unterschiedliche Folgen haben. Dazu zählen Wiederherstellungskosten, Schadensersatzforderungen und Umsatzeinbußen sowie Reputationsschäden. Hinzu kommt, dass es Schadsoftware wie WannaCry darauf anlegt, Lösegelder von betroffenen Unternehmen zu fordern. Hier stellt sich die Frage, wie KMU die konkrete Bedrohungslage wahrnehmen (Abb 4):

Abb. 4 **DsiN-Praxisreport:** Waren Unternehmen bereits von einem IT-Angriff betroffen?



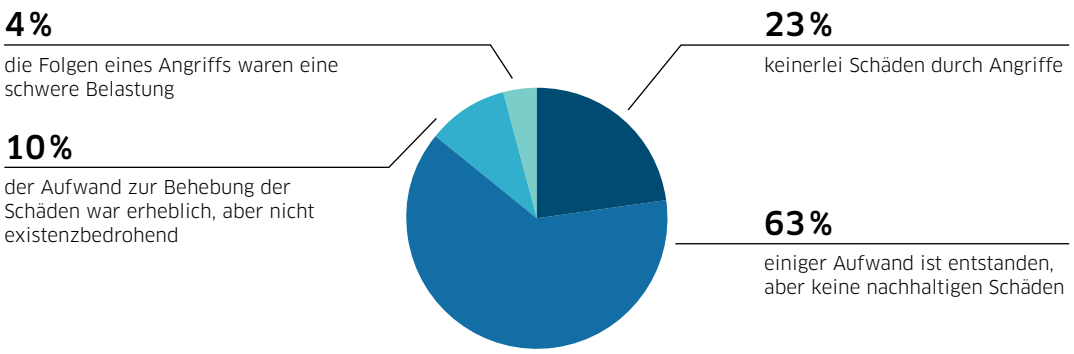

Zwar gibt die Mehrheit der befragten KMU aus ihrer Wahrnehmung heraus an, noch niemals Opfer eines Angriffs geworden zu sein. Dieser Wert ist beachtlich, da die Auswirkungen der Cyberangriffe in der Praxis nicht unmittelbar spürbar zu sein scheinen. Mögliche Ansatzpunkte für eine höhere Sensibilisierung könnten Maßnahmen über typische Angriffsverläufe sein, die auch aus Sicht von Mitarbeitern Relevanz haben und zu höherer Abwehrbereitschaft führen. Beispielsweise aus den Risiken des täglichen Mailverkehrs oder der Verwendung nicht autorisierter Speichermedien im Betrieb.

## 14 Prozent melden erhebliche oder schwere Schäden

Um einen Einblick in die Sicherheits- und Gefahrenlage der KMU zu gewinnen, wurden Unternehmen, die bereits schon mal von einem Angriff betroffen waren, nach den Auswirkungen gefragt (Abb. 5).

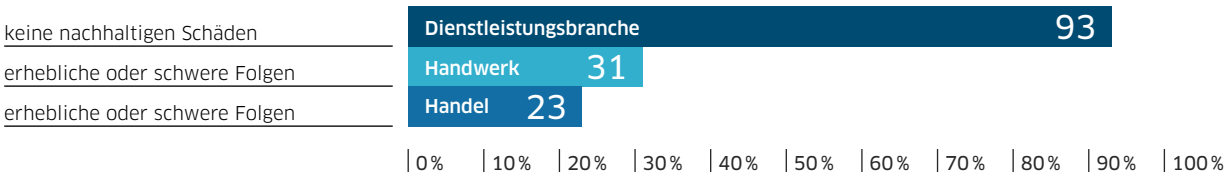
Mehr als drei Viertel der Teilnehmer (77 Prozent) waren infolge der durch Angriffe ausgelösten Schäden mit mindestens einigem Mehraufwand konfrontiert. 15 Prozent der befragten KMU hatten gar mit erheblichen Schäden zu kämpfen. Für den einzelnen Betrieb kann jeder unerwartete Mehraufwand zur Belastungsprobe werden – bis hin zur Beeinträchtigung der Reputation und Wettbewerbsfähigkeit. Auch bleiben Schäden wie der Abzug von Know-how unter Umständen unentdeckt.

**DsiN-Praxisreport:** Wie folgenreich waren Schäden in Folge von Angriffen? **Abb. 5**




Gerade bei der Schadensgeneigtheit von Cyberangriffen könnten darüber Unterschiede zwischen verschiedenen Branchen Rückschluss auf ihre Schutzbedürftigkeit zulassen (Abb. 5a):

**DsiN-Praxisreport:** Die Branchen Handwerk und Handel schneiden am schlechtesten ab – Dienstleistungen am besten: **Abb. 5a**



Eine Betrachtung nach Branchen zeigt, dass von gravierenden Schäden vor allem Handwerk und Handel betroffen sind. Auffällig ist hier die unterschiedliche Wahrnehmung zwischen verschiedenen Branchen. Dieser Befund bekräftigt den Ansatz, digitale Aufklärungsarbeit zielgruppenorientiert nach den spezifischen Bedarfen auszurichten, um individuellen Bedarfen und Sichtweisen besser gerecht werden zu können.

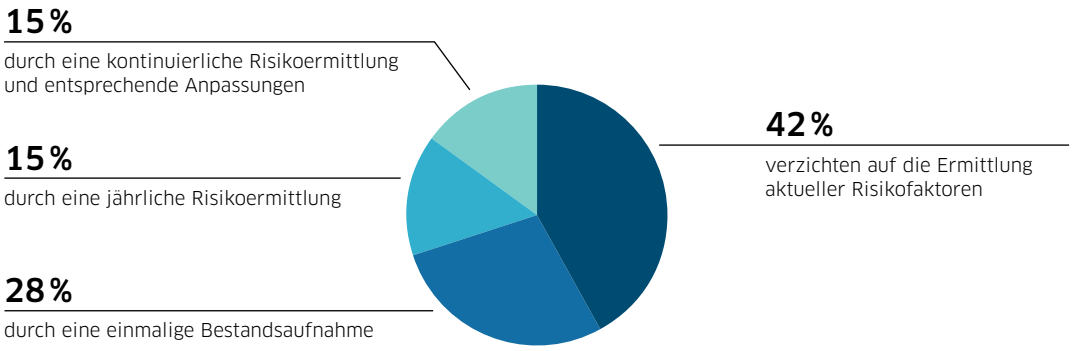
## Schutzbedarf und Risikoanalyse: 42 Prozent ohne jede Risikoermittlung

Mittelständische Unternehmen sind – wie alle anderen Akteure der Digitalisierung – zahlreichen Schadens- oder Angriffsszenarien ausgesetzt: diese reichen von Schäden der Soft- und Hardware über Nachlässigkeiten im Berufsalltag – etwa das leichtfertige Löschen von Daten oder der sorglose Umgang mit firmenkritischen oder personenbezogenen Daten. Bei letzteren stehen mittlerweile zudem empfindliche Bußgelder im Raum. Wenn es um die Sicherheit von Informationen und Systemen geht, ist das richtige Maß an Vorkehrungen gefragt, die sich sich in der Regel nach der Schutzbedürftigkeit orientieren sollten.

Eine Risikoermittlung zeigt dem Unternehmen konkrete Gefahren und Bedrohungen für die Betriebs- und somit auch Wettbewerbsfähigkeit auf. Neben technischen können so vor allem auch menschliche Risiken identifiziert werden. Wie aber steht es um die Analyse der eigenen Risikosituation im KMU (Abb. 6)?

Immerhin 15 Prozent der mittelständischen Unternehmen nutzen die Möglichkeit einer kontinuierlichen Risikoermittlung. Insgesamt 58 Prozent der KMU setzen allerdings – wenn überhaupt – auf eine einmalige Risikoermittlung. Diese ist angesichts rasant wandelnder Angriffsvektoren in der Regel nicht ausreichend. Hier sollte angeknüpft werden, um das Bewusstsein im Mittelstand für die individuellen Risikofaktoren zu stärken – und damit zugleich die damit einhergehenden Sicherheitsmaßnahmen.

**Abb. 6** **DsiN-Praxisreport:** Wie wird die aktuelle Risikosituation überhaupt ermittelt?



# Fazit: Handlungsbedarf bei Risikoeinschätzung

Die Ergebnisse zeigen Nachholbedarf bei der Einschätzung von Risiken durch potentielle Angriffe. Bei den Sicherheitsfragen kommt dem Thema der Wirtschaftsspionage ein besonderer Stellenwert zu: sie erfolgt oftmals durch geschickte Manipulation (Social Engineering), potentiell durch externe aber auch interne Täter. Das Abgreifen von Daten wird darüber hinaus durch den sorglosen Umgang manches Beschäftigten erleichtert (Stichwort ungeschützte Informationen).

Unabhängig von den unmittelbaren Schäden gilt es auch, solche Vorschriften einzuhalten, die wachsende Anforderungen an IT-Sicherheit und Datenschutz stellen. So sehen die neuen Datenschutzregeln strengere Vorkehrungen vor, um die Integrität der personenbezogenen Daten (von Kunden, Lieferanten und Beschäftigten) sicher zu stellen.

### Tipps und Angebote für die Praxis

- Der **DsiN-Sicherheitscheck** bietet einen leichten Einstieg zur Ermittlung des IT-Sicherheitsniveaus in Ihrem Unternehmen. In wenigen Minuten erhalten Sie eine Auswertung mit passenden Handlungsempfehlungen. **www.dsin-sicherheitscheck.de**

- **Mittelstand-Digital** informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Regionale Mittelstand 4.0-Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen. **www.mittelstand-digital.de**

- Der **VdS Quick Check** bietet Ihnen mit 39 Fragen zu sicherheitsrelevanten Themen eine Bestandsaufnahme Ihres Unternehmens. Sie erhalten als Ergebnis eine Matrix, welche die Risikosituation in Ihrem Unternehmen darstellt. **www.vds-quick-check.de**

## Kapitel 2

# Vorkehrungen im Mittelstand: Bedingt abwehrbereit

Die Digitalisierung im Mittelstand schafft neue Angriffsflächen und Gelegenheit für mögliche Beeinträchtigung der IKT in Betrieben. Hinzu kommt eine allgemeine Entwicklung der Sicherheitslage, die von zunehmenden Angriffsaktivitäten und Schäden gerade auch gegenüber der Wirtschaft geprägt ist. Aktuelle Erhebungen wie der BSI-Lagebericht legen nahe, dass diese Bedrohungen sich auch aktuell weiter fortsetzen. Seit Jahren weisen Branchen- und Wirtschaftsinstitute auf Schäden durch Cyberangriffe in Höhe von jährlich 50 Milliarden Euro hin.

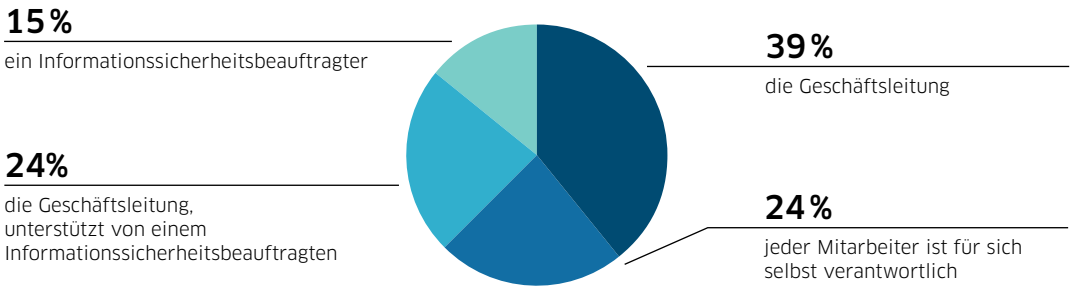
# Nachholbedarf bei Zuständigkeiten und Kompetenzen

**Ein Blick auf die Abwehrbereitschaft des Mittelstands zeigt Schwachstellen sowie auch Bedarfe, die zusätzliche Anstrengungen für mehr IT-Sicherheit erfordern. Es geht um Angriffe nach dem Gießkannenprinzip: Der Großteil der im Umlauf befindlichen und täglich zunehmenden Schadsoftware sucht automatisch nach Schwachstellen in Soft- und Hardware. Aber auch gezielte Angriffe, die auf die größte Schwachstelle der IT, den Menschen, setzen (Social Engineering). Die zunehmende Vernetzung der Wirtschaft zwischen Unternehmen kann die Schadens- und Angriffsrisiken zusätzlich ausweiten.**

## IT-Sicherheit: Geschäftsleitung in 64 Prozent selbst zuständig

Als Einstieg zum Stand der Vorkehrungen des Mittelstands im Umgang mit IT-Sicherheit steht die Zuständigkeit für das Themenfeld innerhalb eines Betriebs (Abb 7):

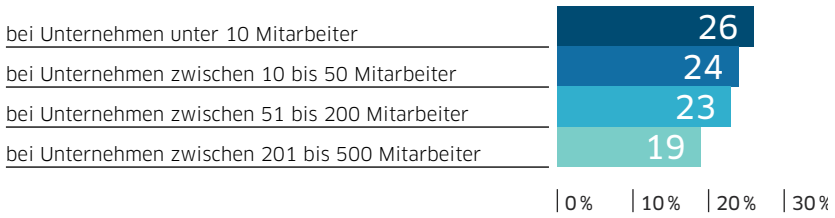
**DsiN-Praxisreport:** Wer ist für die IT-Sicherheit in Ihrem Unternehmen verantwortlich? **Abb. 7**




Die Mehrheit der Befragten gibt an, dass die Verantwortung für IT-Sicherheit bei der Geschäftsleitung liegt – als direkt verantwortliche Stelle oder mit Unterstützung eines IT-Sicherheitsbeauftragten. Bei einem Viertel sind es die Beschäftigten selbst – ein großer Vertrauensvorschuss.

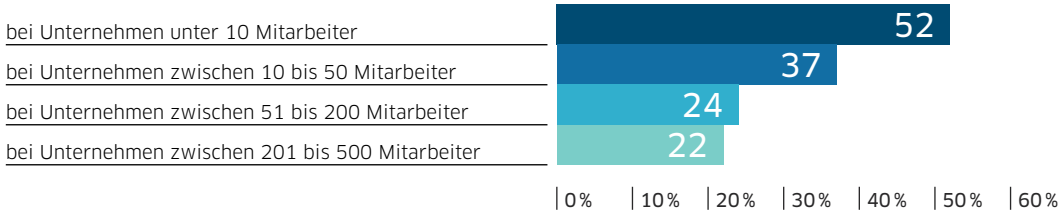
Auch die Differenzierung nach Größe der Unternehmen führt zu einem differenzierten Ergebnis (Abb. 7a):

Abb. 7a **DsiN-Praxisreport:** Unmittelbare Zuständigkeit und Verantwortung der Mitarbeiter selbst für IT-Sicherheit:




Daraus wird ersichtlich, dass die Beschäftigten selbst für die IT-Sicherheit zuständig sind, je kleiner das Unternehmen ist.

Abb. 7b **DsiN-Praxisreport:** Unmittelbare Zuständigkeit und Verantwortung der Geschäftsleitung für IT-Sicherheit:




Es zeigt sich, dass bei Kleinstunternehmen meist die Geschäftsleitung für die IT-Sicherheit unmittelbar zuständig ist (Abb. 7b). Dies könnte durch fehlende Ressourcen begründet sein. Die Devise „IT-Sicherheit ist Chefsache“ ist hier wohl auch auf mangelnde Ressourcen zurückzuführen und bedürfte insoweit eigener Schulungen oder Qualifikationen.

## Entscheidung in Risikosituationen: Zwei Drittel ohne IT-Expertise

Tritt eine Risikosituation ein, ist schneller Handlungsbedarf gefragt, um mögliche Schäden abzuwehren. Alle Mitarbeiter eines Unternehmens sollten informiert sein, was in einer Risikosituation erforderlich ist und wer Ansprechpartner ist. Dies setzt allerdings voraus, dass entsprechende Rollen vergeben wurden und Aufgaben im Falle konkreter Gefahrensituation geklärt wurden (Abb. 8).

Die Geschäftsleitung trifft bei knapp der Hälfte aller befragten Unternehmen die zentralen Entscheidungen. Dies verhält sich analog zu der bereits behandelten Frage, wer für IT-Sicherheit im Unternehmen verantwortlich ist.

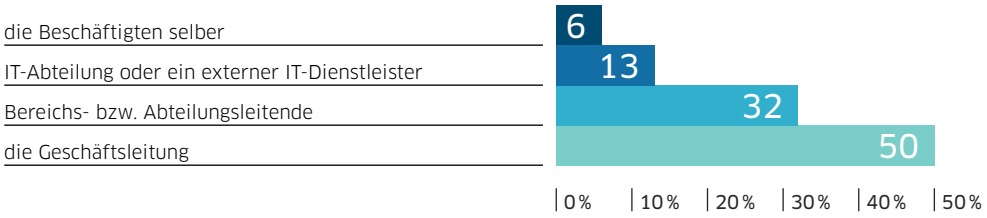
Auch eine genauere Betrachtung entsprechend der Unternehmensgröße führt zu neuen Erkenntnissen (Abb. 8b).

Mit wachsender Größe des KMU sinkt die Anzahl der Unternehmensleiter, die selbst über die operativen Maßnahmen der IT-Sicherheit entscheiden. Bei Kleinstunternehmen mit unter zehn Mitarbeitern beläuft sich dieser Wert auf rund zwei Drittel, und fällt auf einen Wert von knapp unter einem Drittel beim großen Mittelstand ab.

Vor dem Hintergrund muss sichergestellt werden, dass die zuständigen Entscheider ausreichend vorbereitet sind, um auf akute Gefahrenlagen adäquat zu reagieren und umsichtige Entscheidungen zu treffen. Hier besteht gerade bei kleineren Unternehmen Handlungsbedarf, in denen der zuständige Geschäftsführer über keine Expertenausbildung verfügt.

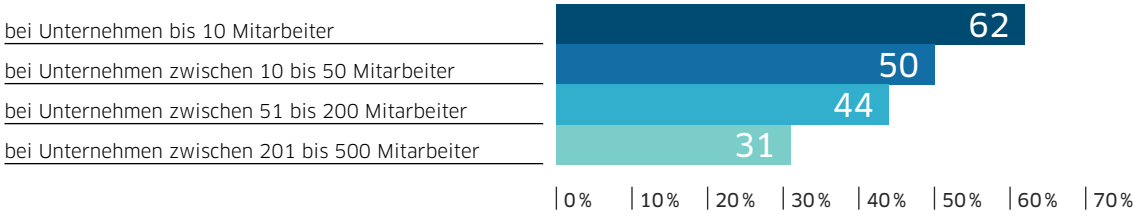
**DsiN-Praxisreport:** Wer im Unternehmen entscheidet über den konkreten Umgang mit Risiken?

**Abb. 8**




**DsiN-Praxisreport:** In welcher Größe Unternehmen entscheidet die Geschäftsführung im Fall einer akuten Bedrohungslage selbst über die operativ durchzuführenden Maßnahmen:

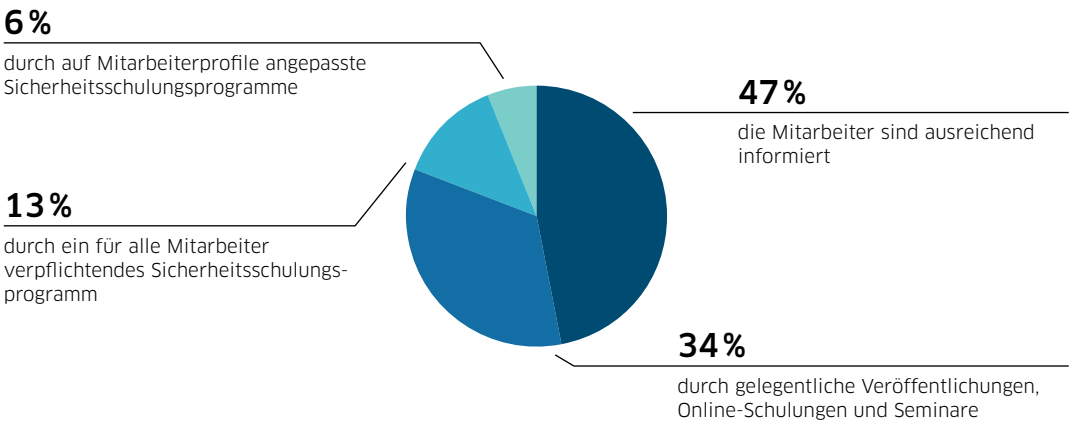
**Abb. 8b**



## IT-Sicherheitsschulungen: Fast die Hälfte ohne Unterstützung

Angesichts der Verantwortung einzelner Mitarbeiter für die IT-Sicherheit ist von Bedeutung, welche Unterstützungs- und Qualifizierungsangebote genutzt werden, um sie für Schutz- und Sicherheitsfragen und Verhaltensweise am Arbeitsplatz zu schulen (Abb. 9).

Abb. 9 **DsiN-Praxisreport:** Auf welche Weise wird eine angemessene Sicherheitskompetenz der Mitarbeiter gewährleistet?




Nicht einmal ein Fünftel aller Befragten setzt auf ein verpflichtendes Sicherheitsschulungsprogramm. Fast die Hälfte geht davon aus, dass Mitarbeiter bereits ausreichend informiert sind. Untersuchungen wie die WIK-Studie[1] deuten darauf hin, dass die meisten Sicherheitsvorfälle durch Beschäftigte verursacht werden. Hier sind zusätzliche Aufklärungsmaßnahmen erforderlich, um Angriffe verlässlich identifizieren zu können. Dieses Bewusstsein muss bei KMU zeitnah verbessert werden.

[1] WIK (2017), Aktuelle Lage der IT-Sicherheit in KMU

# IT-Sicherheitskultur: Jedes dritte Unternehmen verzichtet komplett

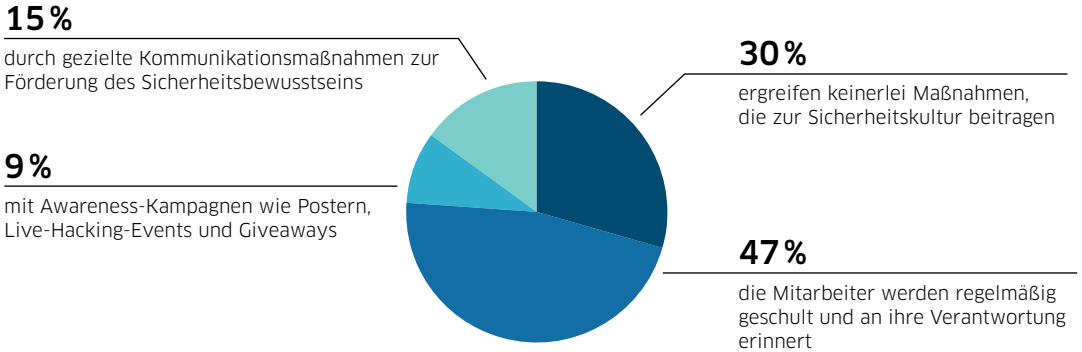
**Das Potential der Einzelmaßnahmen und auch der Prozesse kann nur vollends zum Tragen kommen, wenn IT-Sicherheit auf allen Ebenen und von allen Beteiligten gelebt wird. Damit alle Maßnahmen zusammen die beabsichtigte Wirkung zeigen, ist die gelebte IT-Sicherheit im Betrieb im Sinne einer Sicherheitskultur nicht zu unterschätzen: Eine gelebte Sicherheitskultur im Unternehmen kann auch dazu beitragen, das Unternehmen als zuverlässigen und vertrauenswürdigen Partner im Wettbewerb positiv herauszuheben. Es kommt daher darauf an, was KMU aktiv für eine nachhaltige Sicherheitskultur im Betrieb unternehmen.**

Als Einstieg zum Stand der Vorkehrungen des Mittelstands im Umgang mit IT-Sicherheit steht die Zuständigkeit für das Themenfeld innerhalb eines Betriebs (Abb. 10).

Immerhin fast die Hälfte der Geschäftsleitungen haben Sicherheitsfragen ihre Mitarbeiter im Blick. Allerdings sind vielfältige Maßnahmen erforderlich, um ein mittel- und langfristiges Umdenken und sicheres Handeln bei allen Beteiligten zu bewirken. Hier führen nur 24 Prozent echte Awareness-Aktionen durch oder fördern das Sicherheitsbewusstsein in sonstiger Weise.

IT-Sicherheit kann nur im Dialog mit den eigenen Mitarbeitern hergestellt werden. Auch Nachwuchskräfte gilt es frühzeitig zu sensibilisieren und regelmäßig zu schulen. Dass fast ein Drittel aller Befragten angibt, ohne Sicherheitskultur auszukommen, ist nicht mehr zeitgemäß. Hier ist digitale Aufklärungsarbeit erforderlich, um das Bewusstsein für die Unabkömmlichkeit einer solchen Sicherheitskultur zu verankern. Eine Schulung muss heute längst nicht mehr frontal stattfinden. Partizipative und interaktive Ansätze finden bei Unternehmen immer mehr Anklang.

**DsiN-Praxisreport:** Wie sorgen Unternehmen für eine angemessene Sicherheitskultur? **Abb. 10**



# Fazit: Entscheider für sichere Digitalisierung gewinnen

Der Stellenwert von IT-Sicherheit für die eigenen Betriebsabläufe wird in den Leitungsbereichen der Unternehmen wahrgenommen, auch die Notwendigkeit zu Maßnahmen und Vorkehrungen. Gleichwohl sind Defizite gerade in der organisatorischen Zuordnung von Verantwortlichkeiten und Kompetenzen erkennbar. Es fehlen oftmals Strukturen, die auf aktuelle Sicherheitserfordernisse reagieren und geeignete Maßnahmen gewährleisten. Auch sind Sicherheitskonzepte die Ausnahme, in denen die Rolle der Mitarbeiter und Beschäftigten ausreichend konkretisiert werden. Aktuelle Bedrohungen durch Ransomware oder DDoS-Attacken erhalten dadurch zusätzliche Relevanz.

Wünschenswert wäre eine stärkere Einbindung und Befähigung der Unternehmensleiter, IT-Sicherheit von Anfang in den eigenen Strukturen – sowie auch den Angeboten des Unternehmens – zu etablieren. Künftige Angebote sollten daher einen Fokus darauf legen, Entscheider für diese Herausforderungen zu gewinnen und konkrete Anleitungen zu vermitteln.

### Tipps und Angebote für die Praxis

- DsiN bietet mit **Bottom-Up** ein kostenfreies Bildungsangebot, damit Berufsschulen Auszubildende bereits während der dualen Ausbildung auf die Herausforderungen des Berufslebens vorbereiten können. **www.dsin-berufsschulen.de**

- Mit **Mission: IT-sicher** bietet DsiN eine App, mit der sich alle Beschäftigten mit einem Sicherheitsquiz kurzweilig weiterbilden können. Neben Weiterbildungen sollte die Einführung verbindlicher Sicherheitsrichtlinien in leichter Sprache und Umsetzbarkeit ein weiteres Ziel sein. **www.dsin-berufsschulen/mission-it-sicher**

- Die **Workshopreihe IT-Sicherheit@Mittelstand** von DsiN und dem DIHK zeigt, worauf es bei IT-Sicherheit und Datenschutz in kleinen und mittleren Unternehmen ankommt. Erfahren Sie von Profis, welche Maßnahmen zur Härtung Ihrer IT-Sicherheit in Frage kommen. **www.it-sicherheit-mittelstand.org**

## Kapitel 3

# IT-Schutz in der Praxis: Reaktion und Prävention stärken

Wie bewährt ist die Praxis des Mittelstands im sicheren Umgang mit der Digitalisierung und dem Schutz vor Gefahren? Es geht um die drei Faktoren der Prävention, Detektion und Reaktion, die durch konkrete Maßnahmen mit Leben gefüllt werden.

Abhängig von der Fähigkeit jedes einzelnen Unternehmens, geeignete Vorkehrungen zum Schutz des Betriebsablaufs sicher zu stellen, werden auch die Risiken aus der Digitalisierung kontrollierbar, so dass die Chancen bestmöglich ausgeschöpft werden können.

# Organisatorische und technische Prävention

**Eine robuste IT-Sicherheit erfordert in der Regel einen abgestimmten Prozess, der sowohl organisatorische sowie auch technische und rechtliche Vorkehrungen umfasst. Zu den Aufgaben der Leitungsebene gehört ein dynamisches Risikomanagement, das von der Identifikation von Schwachstellen bis zur Implementierung wirksamer Maßnahmen reicht.**

## Sicherheitsmanagement in KMU: 71 Prozent ohne anerkannte Standards

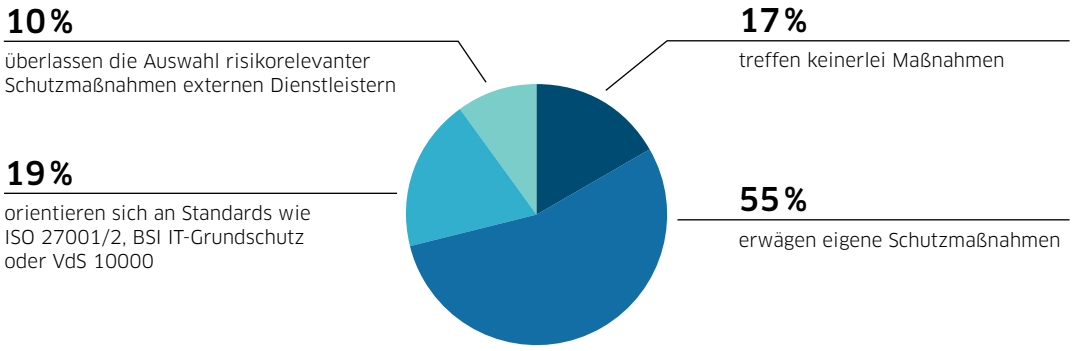
Die frühere DsiN-Studie des Sicherheits-Monitor zeigte über mehrere Jahre eine relativ konstante Zahl von 13 Prozent der Unternehmen, deren Organisationen IT-sicherheitszertifiziert wurden. Wie steht es also um die Situation im Mittelstand der vergangenen 12 Monate (Abb. 11)?

Mit 19 Prozent ist der Anteil derjenigen, die auf bewährte Standards zurückgreifen, erfreulicherweise auf einen höheren Stand als vor zwei Jahren gekommen. Hinzu kommen 10 Prozent der Unternehmen, die für das Thema einen externen Dienstleister einbinden.

Zugleich ist der Anteil an KMU, die eigene Maßnahmen entwickeln, mit 55 Prozent ebenfalls recht hoch. Hier könnten vermeintliche Erwägungen einer Kosten-Nutzen-Kalkulation zu Grunde liegen, Schutzmaßnahmen in weitest gehender Eigenregie zu bewerkstelligen. Die Orientierung an Standards wie dem IT-Grundschutz wäre hier in jedem Fall zu empfehlen. Besser wäre in allen Fällen ein zertifiziertes Management für Informationssicherheit.

Eine Baustelle sind die 17 Prozent der Unternehmen, die auf das Ergreifen jedweder Maßnahme zur Risikominimierung verzichten. Hier ist ebenfalls eine direkte Ansprache im Rahmen digitaler Aufklärungsarbeit erforderlich.

**Abb. 11** **DsiN-Praxisreport:** Wie werden Schutzmaßnahmen im Unternehmen überhaupt identifiziert und bewertet?

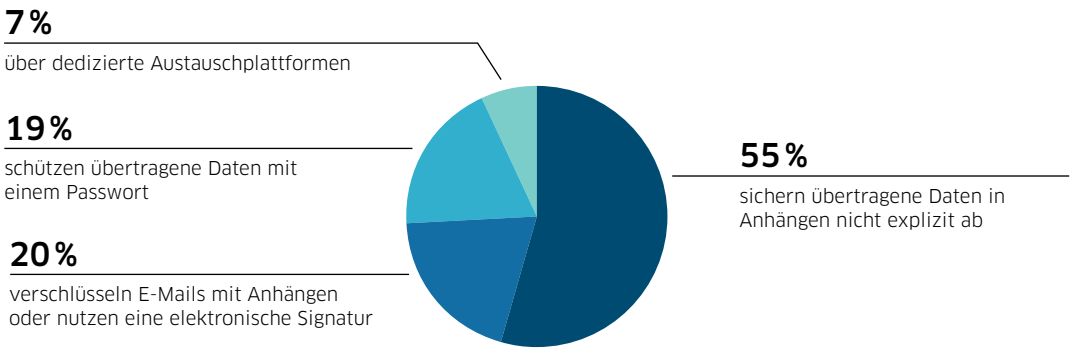


## Schutzmaßnahmen konkret: Sichere Kommunikation bleibt die Ausnahme

E-Mail und Messenger sind wichtiger Gradmesser für die Sicherheit im Unternehmen. Sie sind zugleich die häufigste Form der elektronischen Kommunikation. Der SicherheitsMonitor sah im Jahre 2016 einen großen Nachholbedarf an Sicherheitsvorkehrungen in diesen Bereichen. Für das Jahr 2018 ergeben sich aufschlussreiche Veränderungen (Abb. 12):

**DsiN-Praxisreport:** Welche Schutzmaßnahmen nutzen Unternehmen für den Versand elektronischer Nachrichten mit Blick auf Anhänge?

**Abb. 12**



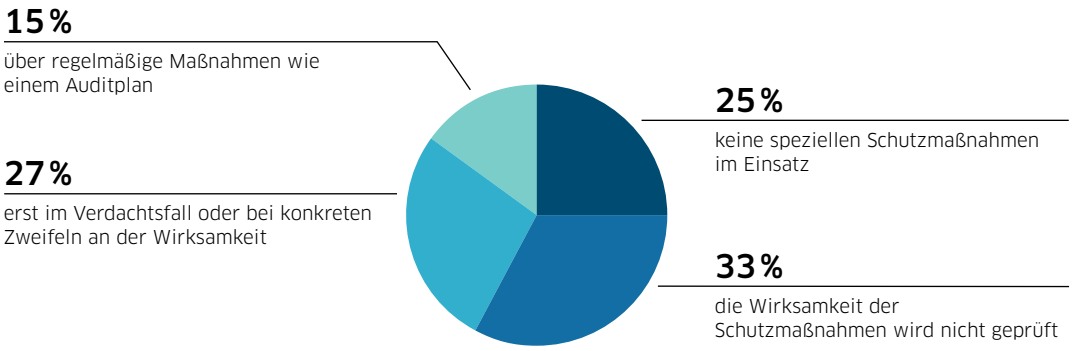

Über die Hälfte der befragten Unternehmen achtet bei der geschäftlichen Kommunikation auf keinen gesonderten Schutz von E-Mails oder elektronischen Anhängen. Ebenso unerfreulich sieht die Lage bei der Verschlüsselung von Anhängen aus: Während im Jahr 2016 nur 15 Prozent der befragten Unternehmen einen Passwortschutz für Dokumente verwendeten, sind es heute immerhin 20 Prozent – ein Plus von fünf Prozentpunkten.

Überraschend, dass nur knapp ein Fünftel der befragten KMU von der Verwendung eines Passwortschutzes für Anhänge und Dokumente beim E-Mail-Versand Gebrauch macht. Diese Vorkehrungen sind sehr einfach umsetzbar und auf fast allen Standardanwendungen verfügbar. Auch zur elektronischen Signatur und der Verschlüsselung sind heute zahlreiche Lösungen verfügbar, wenngleich viele davon für Kleinstbetriebe noch nicht so leicht umsetzbar sind, wie es wünschenswert wäre.

## Wirksamkeit von Schutzmaßnahmen: 15 Prozent mit regelmäßiger Überprüfung

Schutzmaßnahmen können ihre Funktion nur erfüllen, wenn sie wirksam sind – und richtig angewendet werden. Deshalb kommt es auch auf eine regelmäßige Prüfung schützender Maßnahmen und Effekte an (Abb. 13).

Abb. 13 **DsiN-Praxisreport:** Wird die Wirksamkeit von Schutzmaßnahmen im Betrieb überprüft?




Knapp 60 Prozent der Beteiligten prüfen die Effizienz der eingesetzten Schutzmaßnahmen gar nicht oder erst infolge eines Vorfalls. Nur 15 Prozent setzen auf Auditpläne und richten sich demzufolge nach den Kriterien des Qualitätsmanagements. Solange Schutzmaßnahmen nicht auf ihre Wirkung hin getestet werden, bieten sie im besten Fall einen soliden Grundschutz – im schlechtesten jedoch gar keinen. Alarmierend ist, dass viele KMU diesen Ausfall nicht einmal bemerken würden.

Im Sinne eines Qualitätsmanagements und auf Basis von Auditplänen empfiehlt es sich dringend, die Wirksamkeit praktizierter Schutzmaßnahmen regelmäßig zu überprüfen. Dies dient auch der Vertrauensbildung gegenüber Lieferanten. Wie bei den IT-Sicherheitsstandards sind es auch hier vor allem kleine KMU, die praktische Unterstützung – etwa in Form verständlicher Anleitungen – brauchen.

# Schadensvermeidung durch Angriffserkennung

**Das A und O einer effektiven IT-Sicherheitsstrategie ist das rechtzeitige Erkennen von Angriffen. Rechtzeitig heißt, bevor überhaupt ein Schaden entsteht, sei es, dass Informationen oder Systeme beeinträchtigt werden, das Image eines Unternehmens leidet oder Wiederherstellungskosten anfallen.**

## Ein Drittel der Unternehmen ohne Angriffserkennung (35 Prozent)

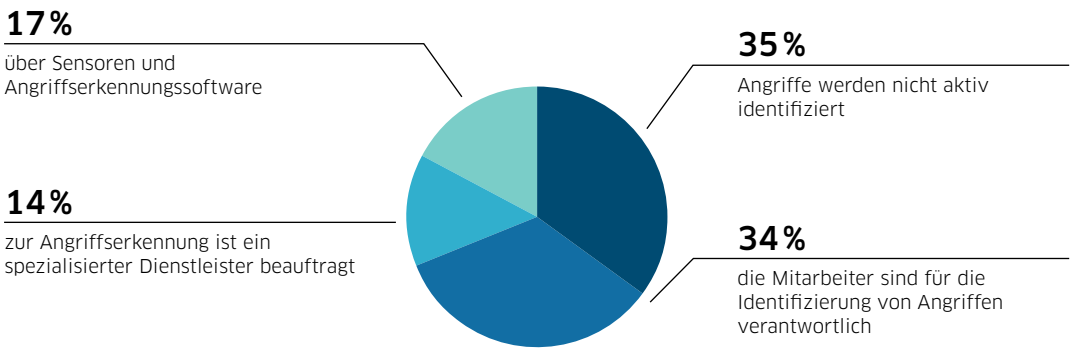
Dank automatisierter Verfahren und entsprechender Technologien wie Antivirensoftware, Firewall oder einem Angriffserkennungssystem (Intrusion Detection System) sind bereits viele Angriffe frühzeitig erkennbar. Wenn sich die Attacken wie beim Social Engineering oder der weiter entwickelten Variante, dem sogenannten Spear-Phishing, jedoch gegen Mitarbeitende und Leitende richten, sind weitere Maßnahmen notwendig.

Vor diesem Hintergrund stellt sich die Frage, auf welche Maßnahmen KMU setzen, um Angriffe überhaupt zu erkennen (Abb. 14).

Knapp mehr als ein Drittel der KMU nimmt bei der Identifikation von Angriffen eine absolut passive Haltung ein. Fast ein ebenso hoher Anteil delegiert diese Verantwortung an die eigenen Beschäftigten. Fast ein Fünftel setzt auf den Einsatz von Angriffserkennungssystemen.

Wenn es um das Erkennen von Angriffen geht, kann Passivität fatale Folgen haben. Auch wenn Angriffserkennungssysteme für bestimmte Betriebsgrößen nicht in Frage kommen, können Dienstleister eingebunden werden, die auf diese Angebote spezialisiert sind. Als Folge der Passivität ist die Dunkelziffer von Angriffen auf Unternehmen ungleich höher als meist vermutet wird. Hier zeichnet sich ein dringender Handlungsbedarf ab, da es sich Unternehmen kaum leisten werden können, bei der Detektion von Angriffen hinterher zu hinken.

Abb. 14 **DsiN-Praxisreport:** Wie erkennen Unternehmen einen Angriff durch oder auf die IT?

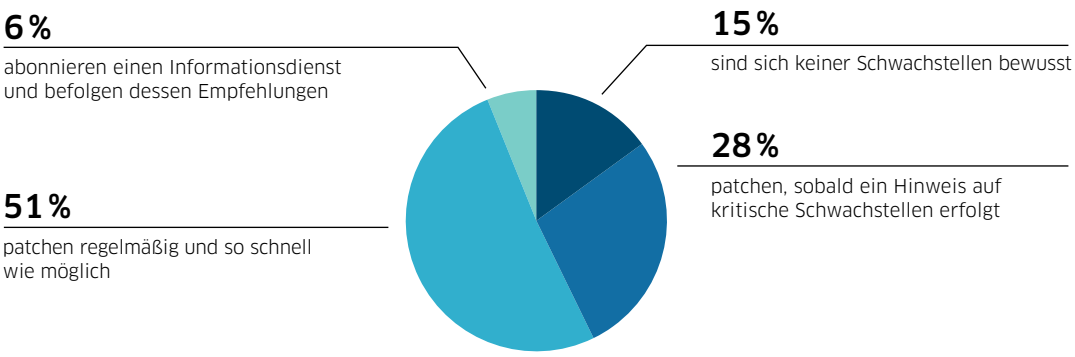


## Schwachstellen in Standardsoftware: Mehrheit patched regelmäßig (85 Prozent)

Hersteller haben ein Interesse, Schwachstellen in Soft- und Hardware zu beheben. In vielen Fällen ist aber eine Mitwirkung der Nutzer erforderlich, um die zur Verfügung gestellten Updates so schnell wie möglich einzuspielen. Der SicherheitsMonitor 2016 stellte fest, dass knapp ein Drittel der KMU keine zeitnahen oder gar keine Aktualisierungen vornahm. Wie steht es um die Patchpraxis der Unternehmen heute (Abb. 15)?

Abb. 15

**DsiN-Praxisreport:** Wie wird mit Schwachstellen in Standardsoftware umgegangen?




Knapp 60 Prozent der befragten Unternehmen greift regelmäßig auf das automatische oder manuelle Aktualisieren zurück oder hat einen speziellen Informationsdienst abonniert. Knapp 30 Prozent der Befragten verlassen sich auf Hinweise seitens der Hersteller oder der Medien.

15 Prozent fehlt das Bewusstsein für die Existenz von Schwachstellen. Auf diesem Gebiet ist es in den letzten zwei Jahren zu keiner signifikanten Verbesserung gekommen. Das bestätigt die passive Haltung im Umgang mit Angriffen. Vor dem Hintergrund, dass sich viele Aktualisierungsvorgänge von Standardsoftware automatisieren lassen, ist hier ein direkter Aufklärungsbedarf erkennbar.

# Schnelle Reaktion im Krisenfall

**Nicht alle Angriffe und Sicherheitsvorfälle können rechtzeitig erkannt und abgewendet werden. Dabei ist im Falle eines Angriffs oder eines Ausfalls der Systeme eine schnelle Reaktion entscheidend, um größeren Schaden zu verhindern. Hier gilt es, den Regelbetrieb schnellstmöglich wiederherzustellen.**

## 23 Prozent verfügen über Notfallpläne oder Ersthelfer

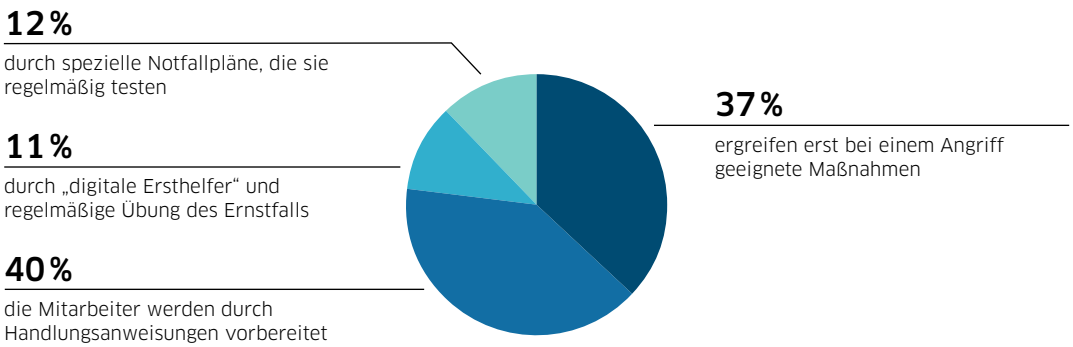
KMU sollten auf den Notfall vorbereitet sein und entsprechende Unterstützungsangebote nach Möglichkeit in Anspruch nehmen, um potenziellen Schäden durch IT-Sicherheitsvorfälle vorzubeugen. Daher ist die Frage zum Umgang mit Notfallplänen entscheidend für den IT-Schutz (Abb. 16).

Erfreulich ist zunächst, dass 12 Prozent über Notfallpläne sowie weitere 11 Prozent der Unternehmen über „digitale Ersthelfer" – also „Feuerwehrleute" für den Ernstfall verfügen. 40 Prozent der Unternehmen geben an, die ausgewählten Beschäftigten für einen Notfall vorbereitet zu haben.

Weit verbreitet unter den KMU ist die Bereitschaft, Risiken einzugehen und es auf einen Angriff ankommen zu lassen – zweifellos eine gefährliche Haltung. Angesichts der zunehmenden Vernetzung mit Zulieferern und Industrie und dadurch wachsenden Anforderungen – auch was die Compliance betrifft - ist eine solche Haltung weder realistisch noch zukunftsfähig.

Bei diesem Thema zeichnet sich dringender Handlungsbedarf ab, Unternehmen in der Erstellung und auch der Ausführung von Notfallplänen zu unterstützen.

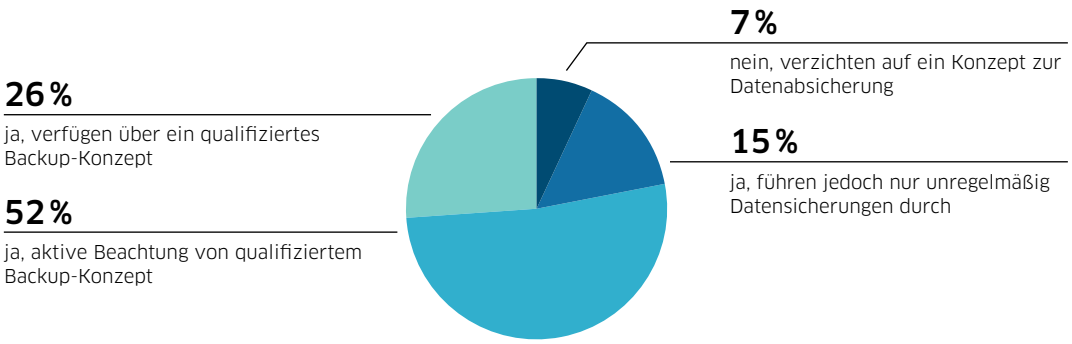
**DsiN-Praxisreport:** Wie reagiert Ihr Unternehmen auf (mögliche) Angriffe? **Abb. 16**



## Wiederherstellung von Daten: 27 Prozent der Unternehmen unzureichend gesichert

Datensicherungen (Backups) sind eine effektive Einzelmaßnahme, um mögliche Schäden nach einem erfolgreichen Angriff einzudämmen – und so im Zweifel sogar die Betriebsfähigkeit aufrecht zu erhalten. Zudem sichern Backups auch gegen die Folgeschäden eines Datenverlusts durch Sorglosigkeiten von Mitarbeitern und höhere Gewalt ab. Datensicherungen sollten daher zum A und O eines jeden Betriebs gehören. Wie sehen das die Teilnehmer dieses Reports (Abb. 17)?

Abb. 17 **DsiN-Praxisreport:** Setzen Unternehmen auf ein Backup-Konzept, um ihre Daten regelmäßig zu sichern?




Über 20 Prozent der untersuchten Unternehmen führen noch keine regelmäßigen Datensicherungen durch oder verzichten vollends auf Backups. Nur ein Viertel testet die Wiederherstellung einzelner Daten. Dies umfasst auch die Einrichtung ausreichender Sicherungsintervalle, die Festlegung der sichernden Systeme, sowie die Art der Datensicherung und Turnus der Wiederherstellungstests.

Was den selbstverständlichen Umgang mit Backups angeht, gibt es derzeit noch viel ungenutztes Potenzial. Angesichts einer zunehmenden Verbreitung von Schadsoftware wie Ransomware und immer ausgeklügelter Angriffe über Social Engineering sollten regelmäßige Datensicherungen für alle Unternehmen in 2018 eine Selbstverständlichkeit sein. Hier besteht Nachholbedarf.

# Fazit: Sicherheitsmanagement stärken – Angebote bereitstellen

Ein Blick auf die konkrete Ausgestaltung der IT-Sicherheitskultur in Deutschland zeigt, dass der Mittelstand verstärkt auf etablierte Standards setzen sollte. Zusätzlich sind Maßnahmen der Detektion und Reaktion erforderlich, etwa in Bezug auf die Befähigung von Mitarbeitern. Nicht zuletzt muss das Thema der Notfallreaktion auf die Agenda. Die fortschreitende Digitalisierung und Vernetzung von Branchen, Zulieferern und Kunden macht wirksame Konzepte für einen systematischen Ansatz praktikabler Maßnahmen unverzichtbar. Passivität kann sich auf diesem Gebiet niemand mehr leisten.

Hier sollten künftig die Leitungen gerade solcher Unternehmen stärker digital sensibilisiert werden, die bislang noch nicht mit der Aufklärungsarbeit erreicht wurden. Zudem geht es um die Ansprache von Mitarbeitern, hier auch der jungen Beschäftigten. Sie können entscheidend zur Abwehr von Gefahren, aber auch dem Ergreifen geeigneter Maßnahmen im Krisenfall beitragen.

### Tipps und Angebote für die Praxis

- Die **SiBa App** von DsiN informiert über sicherheitskritische Vorfälle und stellt erste Handlungsempfehlungen und Sicherheitstipps bereit. Der Informationsdienst ist eine nützliche Quelle, um über aktuelle Risiken informiert zu sein. **www.sicher-im-netz.de/siba**

- Die **Passwortkarte** von DsiN unterstützt eine regelkonforme Passwortbildung und erleichtert das Merken und Aufbewahren von Passwörtern. Die Passwortkarte dient für Unternehmen als Vorlage, um eigene individuelle/persönliche Passwortkarten für die Mitarbeiter zu entwickeln. **www.sicher-im-netz.de/dsin-passwortkarte**

- Der **DsiN-Blog** liefert Expertenbeiträge rund um den sicheren digitalen Geschäftsalltag in kleinen und mittleren Unternehmen. Zahlreiche Gastautoren informieren regelmäßig über aktuelle Entwicklungen hinsichtlich IT-Strategie, Datenschutz, eGovernment oder Cloud Computing. **www.dsin-blog.de**

Kapitel 4

# Geschäftspraxis digital: Relevanz von IT-Sicherheit steigt

Für die Zukunftsfähigkeit des Mittelstands ist der sichere und wettbewerbsorientierte Einsatz digitaler Innovationen entscheidend. Auf diesem Gebiet werden die Anforderungen an IT-Sicherheit und Datenschutz weiter steigen.

Aber auch die Optionen für gelebte Sicherheit im Unternehmen nehmen zu: es geht um technologische Sicherheitsinnovationen, um digitale Aufklärung sowie auch um neue Angebote der Versicherungen, die Risiken absichern können und zur Einhaltung neuer Sicherheitsstandards ermuntern.

# Die vernetzte Wirtschaft

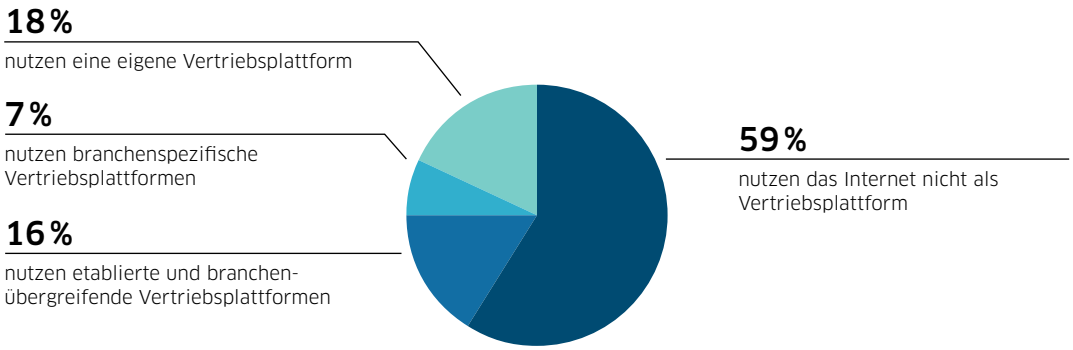
**In einer aktuellen Bestandsaufnahme zeigt der Praxisreport die aktuelle Anwendungsfelder der Digitalisierung, die im Mittelstand zunehmende Verbreitung finden – sowie die einhergehenden Sicherheitsaspekte. Es geht darum, digitale Innovation mit IT-Sicherheit in Einklang zu bringen. Hier sind Entscheider gefragt: denn gelebte IT-Sicherheitskultur hängt direkt von der Praxis ab – sowohl in technologischer als auch organisatorischer Hinsicht.**

## Plattformen: Handel und Vertrieb im Mittelstand

Der Handel über Plattformen sowie die Kooperation unter Partnern und Zulieferern ist ein Treiber der Digitalisierung. Wie aber sieht die Praxis der digitalen Vertriebsstrukturen in Bezug auf Sicherheitsvorkehrungen in der Kommunikation mit Kunden aus (Abb. 18)?

**DsiN-Praxisreport:** Welche digitalen Verkaufsplattformen nutzen Unternehmen – und worauf achten sie in Bezug auf IT-Sicherheitsaspekte?

**Abb. 18**

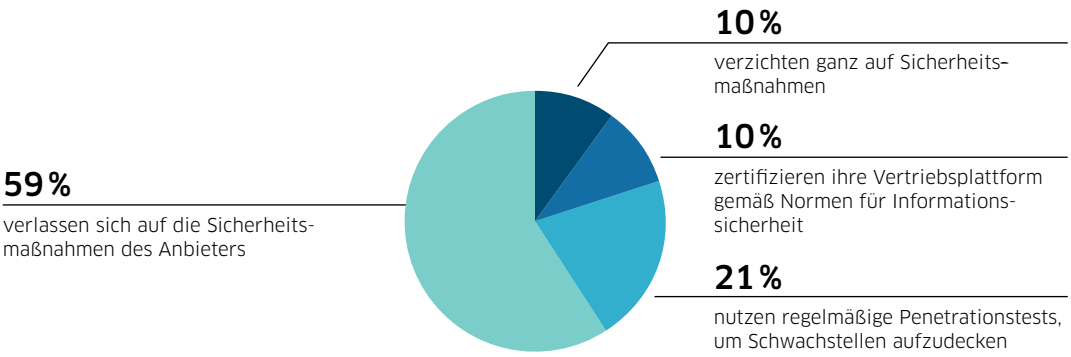



Über 40 Prozent der mittelständischen Unternehmen vertreiben ihre Artikel bereits über Verkaufsplattformen im Internet – fast ein Fünftel nutzt dafür bereits eigene Vertriebsplattformen. Vor dem Hintergrund der an dieser Studie teilnehmenden hohen Anzahl von Kleinstunternehmen (40 Prozent) zeigt sich, dass die Digitalisierung in der gesamten Wirtschaft angekommen ist.

Doch wie sieht es nun beim Vertrieb über Verkaufsplattformen mit den konkreten Sicherheitsvorkehrungen aus (Abb. 19)?

Abb. 19

**DsiN-Praxisreport:** Welche Sicherheitsmaßnahmen setzen Unternehmen bei der Nutzung ihrer Vertriebsplattform ein?




Immerhin führt mehr als ein Fünftel der Befragten regelmäßige Penetrationstests durch. Gerade Kleinstunternehmen profitieren von auf automatisierte Penetrationstests spezialisierten Dienstleistern, mit deren Hilfe sie ihre eigenen Webangebote auf Sicherheitslücken testen lassen können. Mehr als die Hälfte vertraut den Sicherheitsmaßnahmen des jeweiligen Anbieters.

Ein hoffnungsvoller Ansatz ist auch, dass jedes zehnte Unternehmen die eigene Vertriebsplattform zertifizieren lässt. Die Sicherheit und Qualität der eigenen Angebote durch Externe zertifizieren zu lassen, ist jedenfalls ein Vorteil, während mehr und mehr Kunden von Onlineshops auf solche Gütesiegel Wert legen. Genauso so hoch ist jedoch noch der Anteil, der auf entsprechende Sicherheitsmaßnahmen verzichtet. Hier könnte digitale Aufklärungsarbeit sicher weitere Unternehmen für den Weg der Zertifizierung gewinnen.

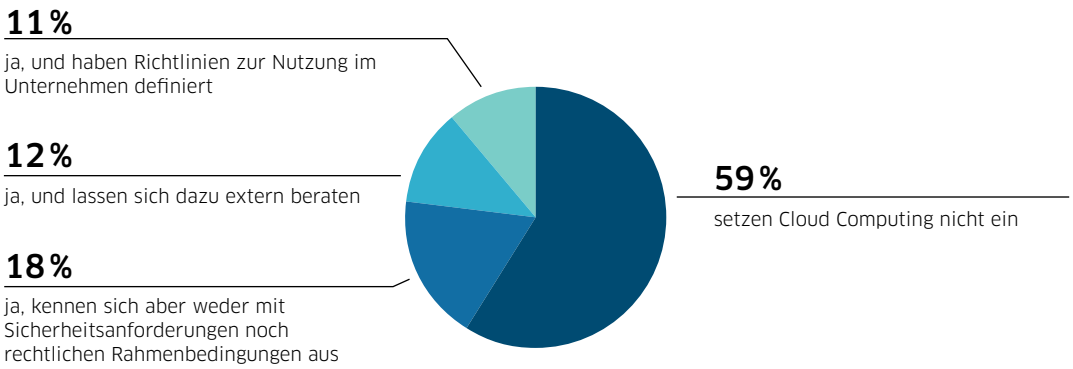
## Cloud im Mittelstand: Vorbehalte und Vorteile

Die Cloud verfügt mittlerweile über vielfältige Angebote für KMU, Betriebsabläufe effektiver und kostengünstiger zu gestalten. Dabei kommt es auch auf die Sicherheit bei der Nutzung an. Der SicherheitsMonitor 2016 kam zu dem Ergebnis, dass hier im Hinblick auf Sicherheitsaspekte und rechtliche Fragen noch erhebliche Unsicherheiten bestanden. Wie verhält es sich damit in 2018 (Abb. 20)?

18 Prozent setzen Cloud Computing ein, kennen sich bei den Sicherheitsanforderungen und rechtlichen Rahmenbedingungen allerdings nicht aus. Die Mehrheit ist auch im Jahre 2018 nach eigener Aussage nicht in der Cloud aktiv. Im Vergleich zu 2016 ist keine signifikante Veränderung zu erkennen. Die Gründe für diese Zurückhaltung sind nicht ohne weiteres ersichtlich. Auch mit Blick auf die neuen Datenschutzregeln, welche die Rechten und Pflichten aus der Nutzung von Cloud Computing neu zuordnen.

Unternehmen müssen sich auf hohe Sicherheitsstandards in der Cloud verlassen können. Dieses Kriterium sollte bei der Wahl eines Cloud-Anbieters die entscheidende Rolle spielen. Standardisierte Vorgaben wie in der „Trusted Cloud“ können hier wichtige Orientierung bieten.

**DsiN-Praxisreport:** Setzen Unternehmen auf Cloud Computing? **Abb. 20**




Cloud-Dienste bedürfen der weiteren Aufklärung hinsichtlich der Sicherheits- und auch der rechtlichen Anforderungen. Hier sind die Unternehmen gefragt, sich aktiv einzubringen. Anbieter und Stakeholder sind gefordert, das Verständnis der Cloud im Mittelstand zu fördern sowie auf ihre Vorteile und Vorbehalte gleichermaßen einzugehen.

## Partner und Zulieferer: Unterschätztes IT-Sicherheitsrisiko?

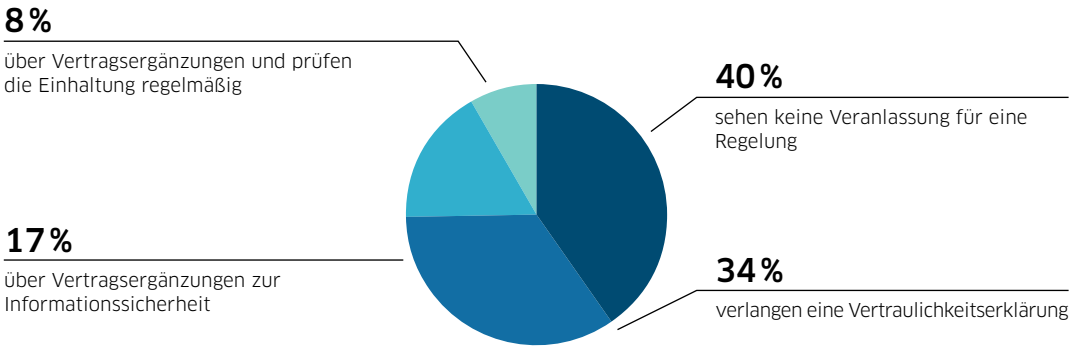
Vor dem Hintergrund der Frage nach entsprechend vertraglicher Regelungen mit Lieferanten und Partnern fragten wir, welche Anforderungen der Mittelstand schon heute in puncto IT-Sicherheit an Lieferanten und Partner stellt (Abb. 21).

Bereits mehr als die Hälfte der KMU verlangt von Lieferanten und Partnern zumindest eine Vertraulichkeitserklärung. Ein Viertel geht sogar schon weiter und verankert das Thema IT-Sicherheit in den Vertragswerken mit Lieferanten und Partnern.

Trotz dieser positiven Entwicklung sehen über 40 Prozent davon ab, sich mit Partnern und Lieferanten auf Regelungen zur Informationssicherheit zu einigen. Hier geht es um ein gemeinsames Fundament zum besseren Verständnis von IT-Sicherheit. Am Ende solcher Prozesse stehen gemeinschaftliche Sicherheitsleitlinien, die für Verbindlichkeit und Transparenz sorgen – und somit für mehr Sicherheit bei allen.

Abb. 21

**DsiN-Praxisreport:** Wie gehen KMU mit Lieferanten und Partnern im Hinblick auf Informationssicherheit um?

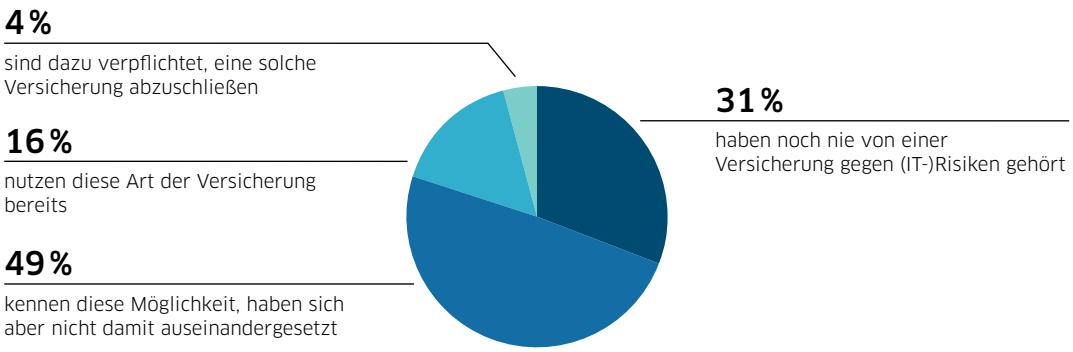


# Cyberversicherungen im Mittelstand

**Die erhöhten Risiken für die Wettbewerbsfähigkeit von Unternehmen, die mit einem möglichen Ausfall oder alleine schon der Beeinträchtigung von Systemen und Daten einhergehen, werfen die Frage nach der Art des Risikomanagements auf. Eine Möglichkeit, die mit der Digitalisierung verbundenen Risiken zu managen, sind Cyberversicherungen. Wie werden diese heute vom Mittelstand in Anspruch genommen?**

**DsiN-Praxisreport:** Haben Unternehmen die Möglichkeit erwogen, eine Versicherung gegen (IT-)Risiken abzuschließen?

**Abb. 22**




Die Mehrheit der befragten KMU (Abb. 22) ist zumindest über die Existenz von Cyberversicherungen im Bilde. Fast ein Drittel der Befragten hingegen hat von einer solchen Möglichkeit noch nie gehört. Es gibt mittlerweile sogar erste KMU, die durch Branchenstandards und Vertragsvereinbarungen zum Abschluss dieser Form der Versicherung verpflichtet sind.

Dass es auf diesem Gebiet weiterhin Aufklärungsbedarf gibt, ist offenkundig. Wie es scheint, haben zwar viele KMU durchaus schon von Cyberversicherungen gehört, sich aber bislang noch nicht mit dieser Möglichkeit auseinandergesetzt. Hier gilt es noch einmal anzusetzen und eine stärkere Auseinandersetzung mit dem Thema anzuregen. KMU müssen über die Vorteile und Kosten von Cyberversicherungen informiert sein. So ist es ein häufiger Trugschluss, dass eine Cyberversicherung bei Fahrlässigkeit im Management oder Berufsalltag greift. Die Partner von DsiN stellen bereits praktische Orientierungshilfen zur Verfügung, unter anderem einen maßgeschneiderten Online-Check und daran anknüpfende detaillierte Informationen.

# Fazit: Digital und IT-Sicherheit gehen Hand in Hand

Der Weg in die Digitalisierung des Mittelstands ist eng verknüpft mit Fragen der sicheren und datenschutzkonformen Umsetzung. Während geschäftliche Entwicklung und Wettbewerbsdruck zu unmittelbaren Veränderungen im Geschäftsbetrieb führen – beispielsweise des Vertriebs über digitale Plattformen – treten Sicherheitsaspekte oftmals erst an zweiter Stelle hervor. Der Report zeigt, dass die Mehrheit bei Innovationen auch grundlegende Sicherheitsaspekte wie das Zertifizieren unterlässt.

Mit der ernsthaften Befassung mit Sicherheitsaspekten im Mittelstand zu ausgewählten Innovationen und Technologien ist auch eine höhere Akzeptanz zu erwarten. So korrespondieren Vorbehalte zur Cloud oftmals mit einer Unsicherheit über rechtliche und technische Voraussetzungen, die erst im Dialog und im Wege digitaler Aufklärungsarbeit geklärt werden können. Das Bewusstsein für sichere Lösungen zu schärfen gilt auch für andere technologische und betriebliche Entwicklungen der Digitalisierung, insbesondere dem verstärkten Austausch zwischen Unternehmen und Partnern im Rahmen einer vernetzten Wertschöpfungskette.

Eine neue Perspektive eröffnet die neue Versicherbarkeit von IT-Risiken in doppelter Hinsicht: sie schützt das Unternehmen vor unerwarteten Schäden und ermuntert zugleich zu einem konkreten Sicherheitsschutz. Das Modell der Versicherungen steckt zwar vergleichsweise noch am Anfang, bietet aber relevante Perspektiven auch für den Mittelstand und kleine Unternehmen.

### Tipps und Angebote für die Praxis

- Der **DsiN-Cloud-Scout** bietet in zehn bis fünfzehn Minuten einen Überblick zu sicherheitsrelevanten Fragen und hilft, die Vorteile von Cloudlösungen sicher zu nutzen.
  **www.dsin-cloudscout.de**

- Mit der **Trusted Cloud** Plattform und dem dazugehörigen Label erhalten Sie einen unabhängigen und transparenten Marktplatz für vertrauenswürdige Cloud Services.
  **www.trusted-cloud.de**

- Der **DsiN Datenschutz-Navigator** zeigt auf, worauf Sie beim Datenschutz achten müssen. Sie erhalten einen ersten Überblick, welche Themen einer zusätzlichen Beachtung bedürfen.
  **www.datenschutz-navigator.org**

## Kapitel 5

# Drei-Punkte-Plan für IT-Schutz im Mittelstand

Die Digitalisierung im Mittelstand als Basis für die Innovations- und Wettbewerbsfähigkeit der Wirtschaft setzt in steigendem Maß Anforderungen an IT-Sicherheit und Datenschutz voraus. Der Praxisreport Mittelstand@IT-Sicherheit zeigt – als Fortführung des DsiN-Sicherheits-Monitor Mittelstand – positive Entwicklung auf, wie die Bereitschaft der Unternehmen zur Zertifizierung von Sicherheitsprozessen.

Andererseits wird deutlich, dass Schwachstellen und Bedarfe in der IT-Sicherheit bestehen, die eine Strategie für eine insgesamt positive Entwicklung zu mehr IT-Sicherheit erfordern. Diese sollen zur Überwindung einer teilweisen Stagnation der Sicherheitsbemühungen und Maßnahmen in Unternehmen beitragen und auf diesem Wege alle beteiligten Akteure einbinden.

# Neue Kultur der IT-Sicherheit – gemeinsam engagieren!

Die gute Nachricht ist, dass die Verfügbarkeit, Zuverlässigkeit und Integrität der Informationssysteme schon heute durch wirksame Maßnahmen verbessert werden können. Es gilt, IT-Sicherheit als Option herauszustellen, für die sich jeder Akteur aktiv entscheiden kann. Die Schaffung eines positiven Umfeldes, das die Herausforderung der IT-Sicherheit und zugleich Lösungsmöglichkeiten aufzeigt, wird die Bereitschaft zu einer gelebten IT-Sicherheit insgesamt vorantreiben.

Diese neue Kultur der IT-Sicherheit bindet alle beteiligten Akteure. Positive Beispiele aus der Wirtschaft wirken als Vorbilder, um auf andere Unternehmen und Partner auszustrahlen. Multiplikatoren im gesellschaftlichen Umfeld und politische Akteure können hier maßgeblich beitragen. Fatalistischen Grundhaltungen („Schutzmaßnahmen nutzen ja sowieso nichts“) werden konkrete Verbesserungen im Wege ausgewählter Sicherheitsmaßnahmen gegenübergestellt und im Dialog vermittelt. Sie fördern die Bereitschaft für veränderte, sichere Verhaltensweisen im Umgang mit IT, die letztlich eine Grundlage für IT-Sicherheit in KMU darstellen.

# Der sichere Weg in die Zukunft – Entscheider gewinnen!

Schutz vor Cyberrisiken wird durch die Entscheider in die Unternehmen eingeführt. Dies gilt sowohl bei kleinen und kleinsten Unternehmen, welche im Praxisreport oftmals auch die unmittelbaren Fachentscheidungen treffen müssen – bis zu großen Mittelständlern, die über die Einführung entsprechender Sicherheitsmanagements zu entscheiden haben. Es liegt daher auf der Hand, den Entscheider im KMU zum Verbündeten für IT-Sicherheit zu machen.

Eine wachsende Aufgeschlossenheit von der Implementierung zertifizierter Sicherheitsstandards in der Organisation über Einzelmaßnahmen bis zur Entwicklung und Produktion neuer Angebote und Dienstleistungen für Kunden und Partner wird sich unmittelbar positiv auf die IT-Schutzfähigkeit auswirken. Erfolgversprechender Ansatzpunkt ist die zunehmende Verschmelzung von Digitalisierung und Geschäftserfolgen auf Grundlage sicherer Geschäftsprozesse, welche für Entscheider damit auch eine betriebswirtschaftliche Dimension erhalten: Wenn IT-Sicherheit Geschäftschancen fördert, ist der Weg zu einer konsequenten und nachhaltigen Härtung der Informationssicherheit im Mittelstand nicht mehr weit.

# Aufklärungsangebote vorantreiben – Akzeptanz stärken!

Eine neue Kultur der IT-Sicherheit und die Einbindung von Entscheidern für mehr IT-Sicherheit im Unternehmen erfordern konkrete Angebote der digitalen Aufklärung, welche die positive Wirkung von geeigneten Maßnahmen aufzeigen und zur Umsetzung ermuntern. Es geht um digitale Aufklärung zu sicheren Verhaltensweisen, aber auch die Befähigung, technologische Maßnahmen zu ergreifen oder zu veranlassen. Initiativen nach dem Gießkannenprinzip scheinen auf den ersten Blick zwar viele Menschen anzusprechen, sind in der Regel aber wirkungslos im Sinne der IT-Sicherheit.

Es geht um einen echten Dialog, der bei den Mitarbeitern und Entscheidern ankommt. Hier ist zusätzliches Engagement aller Beteiligten gefragt, um die entsprechenden Angeboten auf den Weg zu bringen. Aber auch auf Seiten der Adressaten wird es darauf ankommen, die Angebote anzunehmen und im Umfeld der Betriebe zu verbreiten. Nicht zu unterschätzen ist der Effekt eines sicheren Mittelstands auch auf die Resilienz der gesamten Gesellschaft und Wirtschaft, wenn der sichere Umgang mit der Digitalisierung im Betriebsalltag erst einmal zur Selbstverständlichkeit wird.

Zur Identifikation relevanter Themenwelten aus dem Bereich des Mittelstands, sowie auch passender Partner und Zielgruppen zur Vermittlung der Aufgaben hat DsiN im Herbst 2018 einen *Deutschland Dialog für digitale Aufklärung* gestartet, der zur Teilnahme aller Partner einlädt, die IT-Sicherheit als Grundlage einer erfolgreichen Digitalisierung im Mittelstand verstehen.

# **DsiN-Praxisreport** Mittelstand@IT-Sicherheit **2018**

## Zentrale Ergebnisse

- ✔ Abhängigkeit von IT-Sicherheit steigt – Aber: keine organisatorischen Reaktionen
- ✔ Mittelstand fürchtet Cyberangriffe – Aber: Schutzvorkehrungen bleiben aus
- ✔ IT-Sicherheit ist machbar – Aber: fatalistische Haltungen hemmen

## Der Drei-Punkte-Plan

| | | |
|---|---|---|
| 1. | **Schaffung einer IT-Sicherheitskultur** | Bewusstsein und Offenheit für neue Wege der IT-Sicherheit |
| 2. | **Entscheider für IT-Sicherheit gewinnen** | IT-Schutzvorkehrungen für Betrieb, Mitarbeiter und Partner |
| 3. | **Aufklärung vorantreiben Akzeptanz stärken** | Geschäftsbetrieb und IT-Sicherheit gehen Hand in Hand |

## Digitale Transformation gründet auf IT-Sicherheit!

# Deutschland sicher im Netz e.V.

DsiN leistet konkrete Hilfestellung für Verbraucher sowie für kleine und mittlere Unternehmen im sicheren Umgang mit dem Internet. Dafür entwickelt DsiN praktische Angebote und Anleitungen im Verbund mit Unternehmen, Verbänden und Vereinen. ls produktunabhängige Plattform für Aufklärungsinitiativen ist DsiN für neue Mitglieder offen, die IT-Sicherheit als maßgeblich für den Erfolg der Digitalisierung betrachten.

In der Digitalen Agenda der Bundesregierung wurde ein Ausbau der Zusammenarbeit und Unterstützung von DsiN beschlossen. Schon heute verstärkt DsiN seine Aufklärungsarbeit:- Für Verbraucher stehen kostenlose Anleitungen zum souveränen digitalen Umgang im Netz im Mittelpunkt wie die SiBa-App zu aktuellen Warnmeldungen und das DsiN-Webportal.

Gegründet wurde DsiN als gemeinnütziger Verein im Nationalen IT-Gipfelprozess der Bundesregierung und steht seit 2007 unter der Schirmherrschaft des Bundesministeriums des Innern. DsiN möchte seine Aufklärungsarbeit im Dialog mit der Politik, der Wissenschaft und weiteren Akteuren der digitalen Gesellschaft weiter stärken.

# Impressum

## DsiN-Praxisreport Mittelstand@IT-Sicherheit

Studie von Deutschland sicher im Netz e.V. zur digitalen Sicherheitslage der kleinen und mittleren Unternehmen in Deutschland

**Verantwortlich:** Dr. Michael Littger
**Redaktion:** Marc Gawron, Piet Simon, Sascha Wilms
**Gestaltung und Grafik:** Thomas Heidtmann | www.thomasheidtmann.com
**Quellennachweise:** SAP, DsiN, Titel/Seiten 8, 15, 21, 30, 36 de.fotolia.com
**Stand:** November 2018

Deutschland sicher im Netz e.V.
Albrechtstraße 10 b
10117 Berlin
Telefon +49 30 27576 – 310
Telefax +49 30 2757651 – 310
www.sicher-im-netz.de
info@sicher-im-netz.de

Ein Handlungsversprechen von: